



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/536,053	03/27/2000	Michael K. Just	0500.9912151	5651
23418	7590	08/22/2006	EXAMINER	
VEDDER PRICE KAUFMAN & KAMMHOLZ 222 N. LASALLE STREET CHICAGO, IL 60601			ZAND, KAMBIZ	
			ART UNIT	PAPER NUMBER
			2132	

DATE MAILED: 08/22/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/536,053

Applicant(s)

JUST, MICHAEL K.

Examiner

Kambiz Zand

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 16 June 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-7, 9-15, 17-26, 28-35, 37, 38 and 44-46 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☒ Claim(s) 40-44 is/are allowed.
- 6) ☒ Claim(s) 1-7, 10, 12, 14, 17, 18, 20-26, 29-35, 38 and 45-46 is/are rejected.
- 7) ☒ Claim(s) 9, 11, 13, 15, 19, 28 and 37 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

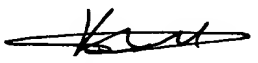
Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 27 March 2000 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.


KAMBIZ ZAND
PRIMARY EXAMINER

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

1. The text of those sections of Title 35, U.S. Code not included in this section can be found in the prior office action.
2. The prior office actions are incorporated herein by reference. In particular, the observations with respect to claim language, and response to previously presented arguments.
3. New claim 46 has been added.
4. Claims 1-7, 9-15, 17-26, 28-35, 37-38 and 40-46 are pending.

Claim Objections

5. Claim 45 is objected to because of the following informalities: the phrase "friendly" is a relative term. Appropriate correction is required.

Response to Arguments

6. Applicant's arguments filed 06/16/2006 have been fully considered but they are not persuasive.
 - Applicant response on page 14, and page 15 (lines 1-16) includes applicant's interpretation of the references used in the application.
 - As per applicant's arguments that Geist do not describe "digital signature verification error determination in the cited portions of Gist", examiner makes the following remarks:

a) Generation of the digital signature by public key cryptography is well known in the art, which is signing a document using a private/public key. Therefore based on such basic understanding that one should consider the references used in the rejection.

b) Gist disclose on fig.2 generation of the digital signature and storing of the signature. On fig.3, retrieve the public key, check for authenticity through the public key certificate where the owner is the identifier of the public key and after authenticity, make a digital signature verification to see the authenticity of the signature, which corresponds to digital signature verification error of the applicant. Examiner had the option to claim inherency with respect to step 303 and 311 of the "association of the public key with the digital signature" since absent of such association would result in non-authentication of the digital signature. However examiner has used obviousness rejection in order to avoid ambiguity with respect to message header identifier association with public key certificate identifier (please see generation of digital signature using public key crypto concept by searching google). Having said that Examiner still maintains the rejection based on the references used and the motivations to combine.

c) Col.4, lines 45-67 disclose directory that uses the tag to locate the public key certificate (certificate is in the form of data, data is in the form of contents, when transmitted has a header and the payload, the basic of data transmission in the network), and then locate the corresponding digital signature; col.5-col.6, line 38 disclose not only generation of the digital signature and generation of the public

key certificate, but also how the digital signature being authenticated, that is the mapping of the certified public key corresponding to the digital signature associated with. It is obvious if a non-associated public key is presented it result in an error with respect to such mapping.

Applicant has provided any arguments with respect to why such combination of the references does not disclose applicant's invention in a rational manner.

Therefore:

In response to applicant's (overall) arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

Claim Rejections - 35 USC § 103

7. **Claims 1-7, 10, 12, 14, 17, 18, 20-25, 29-35 and 46** are rejected under 35 U.S.C. 103(a) as being unpatentable over Geist (6,757,827 B1) in view of Schmeidler et al. (6,763,370 B1); and further in view of Bisbee et al (6,367,013 B1).

As per claims 1, 17, 20 and 29 Geist discloses the determination of a digital signature verification error (see abstract; see fig.2-3 and associated text; col.2, lines 44-62) and the generation of a digital signature verification map (see col.4, lines 45-67; col.5-col.6,

Art Unit: 2132

line 38; fig.1-3) but do not explicitly disclose association of the digital signature with corresponding public key (generating digital signature using public key). However Schmeidler et al. (6,763,370 B1) disclose association of the digital signature with corresponding public key (generating digital signature using public key) see col.26, lines 55-59). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Schmeidler's public key digital signature algorithm in Geist's method, apparatus and storage medium's signature verification method steps and means in order to provide security to protect the value of the content and prevents unauthorized use and copying thereof (see schmeidler col.2, lines 21-23). Geist in view of Schmeidler et al do not disclose received message header identifier association with public key, digital signature entity and the mapping.

However Bisbee et al (6,367,013 B1) disclose header identifier association with public key, digital signature entity and the mapping (see fig.1a, 23A4a and 5a and associated texts). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Bisbee et al 's digital signature chaining in Geist's method, apparatus and storage medium signature verification method steps and means in view of Schmeidler's public key digital signature algorithm in order to re-validate e-original object a current time stamp and digital signature and current authentication certificate.

As per claims 2, 5, 21, 24, 30, and 33, in addition to the teachings applied above, Geist discloses the storage, receipt, and digital signature verification map update of at

Art Unit: 2132

least one acceptable message header identifier, which becomes a map entry (see fig.2-3).

As per claims 3, 22, and 31, in addition to the teachings applied above, Geist discloses that the generation step includes mapping the plurality of acceptable message header identifiers on a per certificate subject identification basis (see fig.1-3; col.3-5).

As per claims 4, 10, 12, 18, 23, and 32, in addition to the teachings applied above, Geist discloses the verification of a digital signature associated with received message information (see fig.2-3 and associated text).

As per claims 6, 14, 25, and 34, in addition to the teachings applied above, Geist discloses that the message header identifier includes at least one of data representing a sender's email address, telephone number, and unit identifier (see fig.1-3 and associated text).

As per claim 7, 26 and 35 Geist (6,757,827 B1) discloses the determination of a digital signature verification map to provide a trusted digital signature verification map (see fig.2-3).

As per claim 46 Geist (6,757,827 B1) disclose the method of claim 1 comprising continually updating the digital signature verification map to accommodate aliases to common subject associated with the certificate (see col.5-6 line 38).

8. **Claims 38 and 45** are rejected under 35 U.S.C. 103(a) as being unpatentable over Geist (6,757,827 B1) in view of Schmeidler et al. (6,763,370 B1) and further in view of Bisbee et al (6,367,013 B1) as applied to claims 1 , 10, 20, and 29 above, and further in view of Cooper et al (US006O52442A).

As per claim 38 Geist in view of Schmeidler and further in view of Bisbee discloses the determination of a digital signature verification error (see as applied to claim 1 above) and the generation of a digital signature verification map (see as applied to claim 1 above). Geist also discloses the storage, receipt, and digital signature verification map update of at least one acceptable message header identifier, which becomes a map entry (see as applied above). Chan et al additionally discloses the verification of a digital signature associated with received message information (see as applied above). Geist in view of Schmeidler in view of Bisbee fails to expressly disclose the generation of a trusted alias map and the display of at least one subject alias. However, Cooper et al discloses these features (see the directory "display" and "mnemonic tag" in Cooper et al--page 9, first column, second and sixth paragraphs and column 10, first paragraph). Therefore, it would have been obvious to one of ordinary skill in the art at the

time the invention was made to modify the method of Geist in view of Schmeidler by generating a trusted alias map relating to corresponding mnemonic aliases of Cooper and by displaying these aliases in place of the same URLs and sender email addresses.

One of ordinary skill in the art would have been motivated to do so in order to facilitate the identification of Geist's message sources in view of Schmeidler.

As per claim 45 the use of e-mail address that corresponds to an entity is well known in the art, therefore proper certificate of an entity association with an e-mail is also obvious. The claim also shows an intended use (A recitation directed to the manner in which a claimed apparatus is intended to be used does not distinguish the claimed apparatus from the prior art if prior art has the capability to do so perform (See MPEP 2114 and Ex Parte Masham, 2 USPQ2d 1647 (1987))).

Allowable Subject Matter

9. Claims 40-44 are allowed.

10. Claims 9, 11, 13, 15, 28 and 37 would be allowable if rewritten to include all of the limitations of the base claim and any intervening claims.

Conclusion


11. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kambiz Zand whose telephone number is (571) 272-3811. The examiner can normally be reached on Monday-Thursday (8:00-5:00). If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone numbers for the organization where this application or proceeding is assigned are 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR

Art Unit: 2132

or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



KAMBIZ ZAND
PRIMARY EXAMINER

08/16/2006

AU 2132